Vulnerability Concepts and Models

Research in Progress

Dr. Adrian V. Gheorghe

Batten Endowed Chair of

Systems Engineering

My Personal Experience

- Vulnerability Switzerland
- Vulnerability Assessment Petrochemicals and Refineries – SwissRe
- Energy Security – Black Sea Area
- Vulnerability Assessment – Critical Infrastructures/System of Systems Approach – USA

The relevance towards a comprehensive approach to QVA

Journal of Risk Research
Volume 7 Issue 6 September 2004 ISSN: 1366-9877

Special Issue: Risk and vulnerability of critical infrastructure

1366-9877(2004)7:6;1-C

Carfax Publishing
Taylor & Francis Group

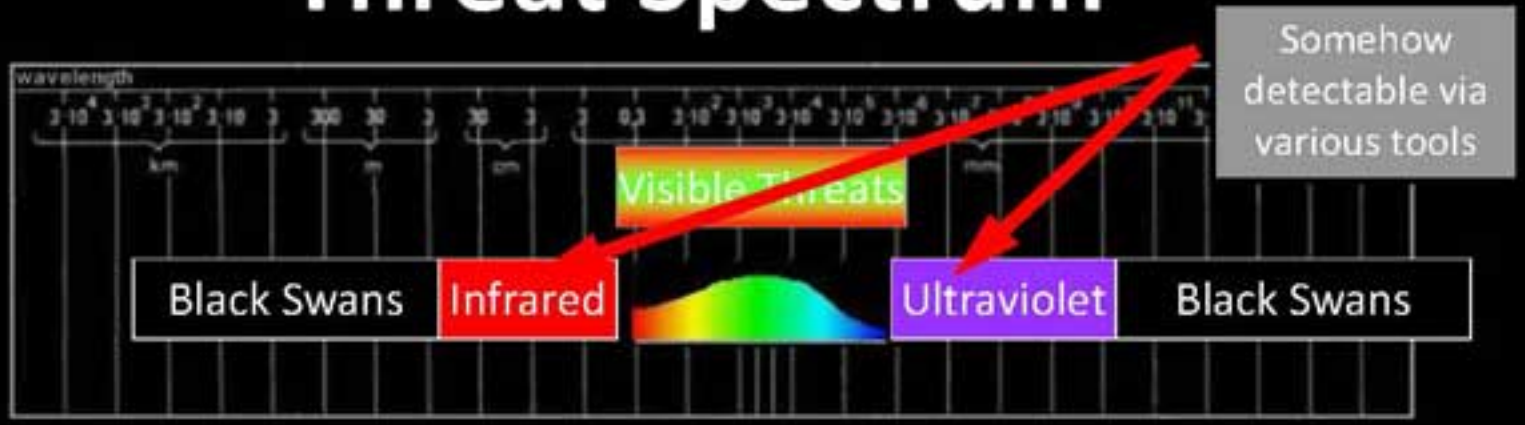
Outline

- **Part I**
  - Vulnerability, what is it?
  - Factorization of Homeland Security
  - Risk vs. Vulnerability
- **Part II**
  - Quantitative Vulnerability Assessment – A Complex Landscape

Factorizing Homeland Security

- Risk
- Vulnerability
- Threat Spectrum

Threat Spectrum



Visible Threats

- ABC of threats → Conventional Threat/Risk Managements
  - Atomic, Biological, Chemical, Drugs, Epidemics, Finance, Global Warming, Information Security, etc…
- Ultraviolet – Infrared Threats
  - Implementing New Technology (i.e. Autonomous Aircraft Systems)
- Black Swans (Only visible once revealed)
  - Ambiguous Threats (i.e. Nanotechnology)
  - Completely Unexpected Threats (i.e. 9/11)

Revealing Threats Over Time

…How About Changing Trends and Definitions?

- **Web 2.0**
- **Democracy 2.0**
- **Threat 2.0**
- **Resiliency 2.0**

Part One

Vulnerability: Topic in Debate

Secretary Napolitano Issues First in a Series of Action Directives

- **Critical infrastructure protection**: This core mission of DHS entails a broad mandate to reduce the ***vulnerability*** of key systems and structures to natural and manmade threats…

- **Risk analysis**: Given the extensive number of ***vulnerabilities*** to manmade and natural disasters and the limitations on resources, determining national priorities and the judicious distribution of resources are a major element of the department's mission.

•According to National Infrastructure Protection Plan (NIPP)

Risk = Consequence x Vulnerability x Threat

Vulnerability: Physical ***feature*** or ***operational attribute*** that renders an entity open to exploitation or susceptible to a given hazard.

Threat: Natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Consequence : The effect of an event, incident, or occurrence; reflects the level, duration, and nature of the loss resulting from the incident.

National Infrastructure Protection Plan

Partnering to enhance protection and resiliency

2009

Vulnerability Definition Landscape (1)

- **Computer Science:** *A **weakness** in a computing system that can result in harm to the system or its operations, especially when this weakness is exploited by a hostile person or organization or when it is present in conjunction with particular events or circumstances.*

- **Thesaurus:** **[Vulnerability is]** *the **condition** of being laid open to something undesirable or injurious: exposure, liability, openness, susceptibility, susceptibleness, vulnerableness.*

Vulnerability Definition Landscape (2)

- **Military Vulnerability:** A subset of Survivability (the others being **Susceptibility** and **Recoverability**). Vulnerability is defined in various ways depending on the nation and service arm concerned, but in general it refers to the near-instantaneous effects of a weapon attack. In some definitions Recoverability (damage control, firefighting, restoration of capability) is included in Vulnerability.

- **Invulnerability/Invulnerability:** A common feature found in video games. It makes the player impervious to pain, damage or loss of health.

Vulnerability Definition Landscape (3)

- **Generic Vulnerability**: The **susceptibility** to physical or emotional injury or attack. It also means to have one's guard down, open to censure or criticism; assailable. Vulnerability refers to a person's state of being liable to succumb, as to persuasion or temptation. (The Free Dictionary http://www.thefreedictionary.com/vulnerability)

So, What Does Vulnerability Mean?

- No clear definitions
- Late latin word "vulnerabilis"
  - **the capacity to be physically or emotionally wounded or hurt**
  - **vulnerability indicates *a state* that predisposes people or places to hazards**
  - ***Openness* to physical injury or attack**
- Common understanding
  - *f* {susceptibility, resilience}
- Working definition
  - "Vulnerability is a system's virtual openess to lose its design(ed) functions, and/or its structural integrity or identity"[AVG]

Susceptibility and Resilience

- **Susceptibility** is a trait, an inherent property of a system. Its synonym is called proneness

- **Resiliency** comprises protection and adaptation/regeneration power of the system to induced changes or pertubation.
  - Its synonyms are
    - Robustness
    - Adaptibility
    - Flexibility
    - Plasticity
    - Stability

Risk

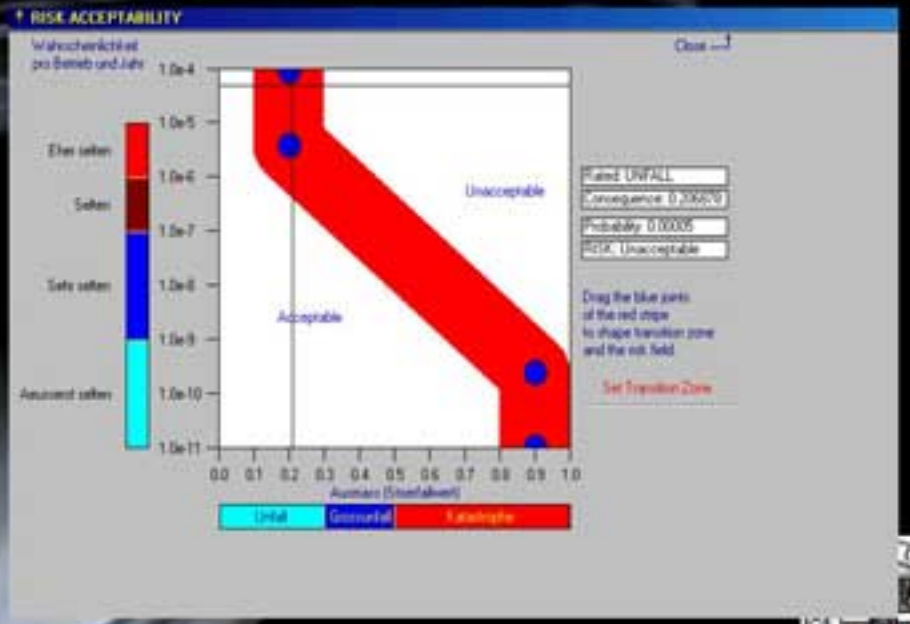
... is a construct, defined as:

Risk = Probabilities x Consequences$^{\alpha}$

... visualized with a Risk Matrix and (ALARA) As Low as Reasonably Achievable

Risk Perception

- ***Low Probability vs. High Consequence***
- ***High Probability vs. Low Consequence***



Vulnerability

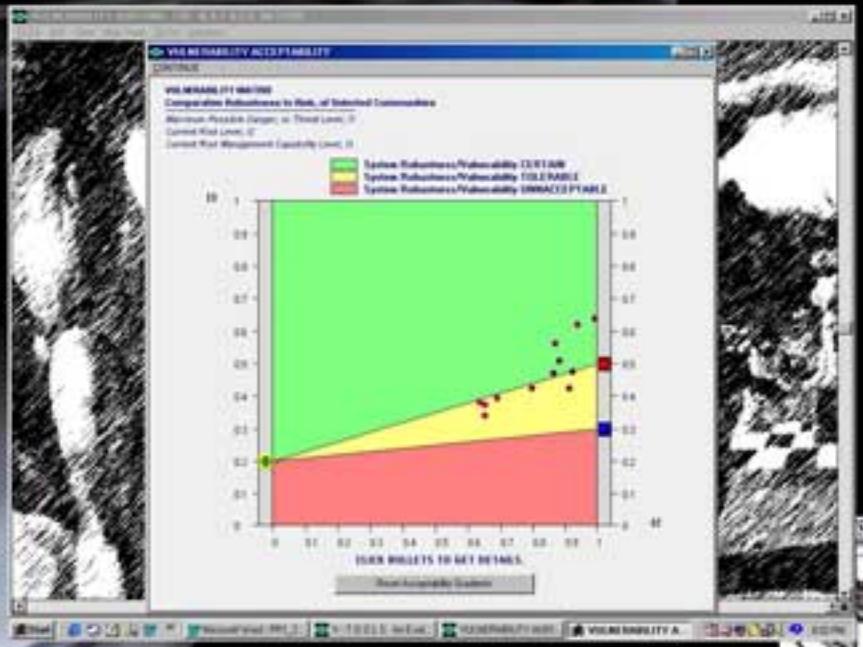
... is ***NOT*** a construct, it is a System State:

Vulnerability= f (Susceptibility, Resilience)

... visualized with a Vulnerability Matrix and (ARASP) As Resilient as Society/System Permits

Vulnerability Perception

- ***Low Susceptibility vs. High Resilience***
- ***High Susceptibility vs. Low Resilience***



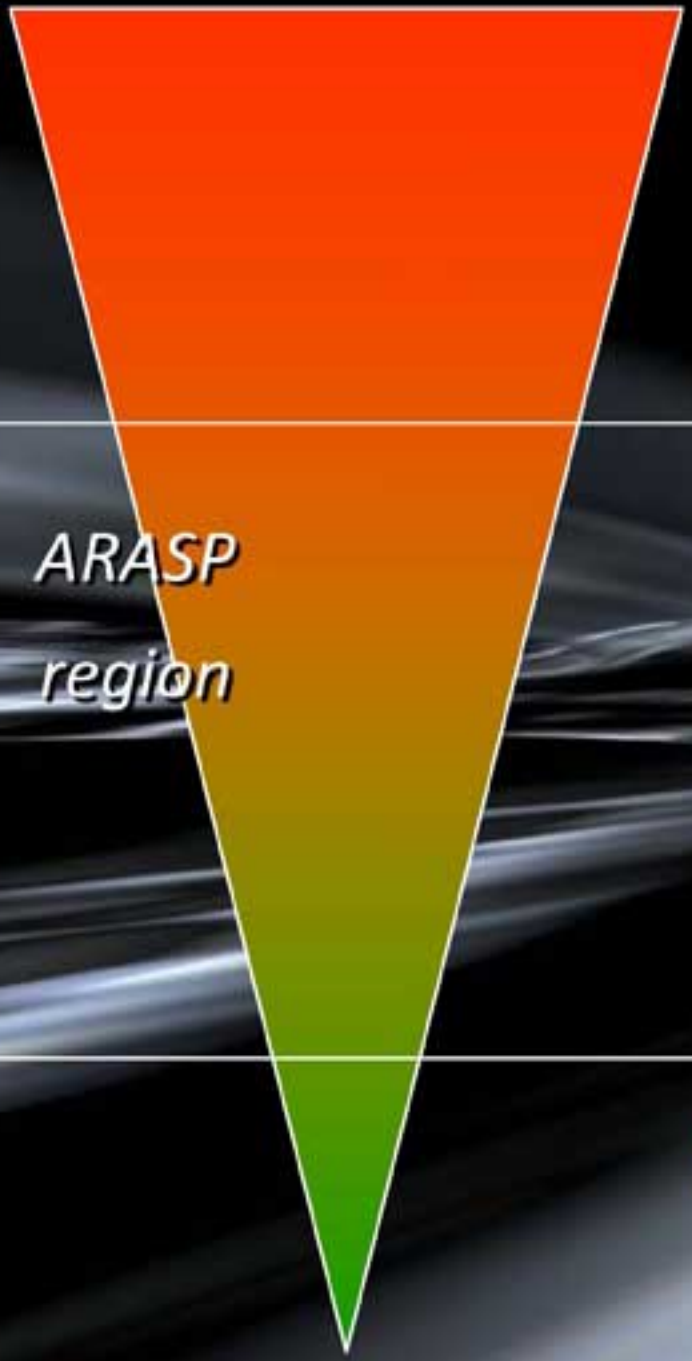
AS LOW AS REASONABLY ACHIEVABLE (ALARA)

Risk intolerable and I cannot be justified even in extraordinary circumstances

Risk is tolerable only if mitigation methods are impracticable or if its cost is grossly in disproportion to the improvement gained

Tolerable if cost of reduction would exceed the improvements gained

No need for detailed studies. Check that risk maintains at this level



AS RESILIENT AS SOCIETY (SYSTEM) PERMITS (ARASP)

Vulnerability intolerable, vulnerability cannot be justified even in extraordinary circumstances

Tolerable only if vulnerability reduction is impracticable or if its cost is grossly in disproportion to the improvement gained

Tolerable if cost of reduction would exceed the improvements gained

No need for detailed studies. Check that vulnerability maintains at this level

Risk vs. Vulnerability

Risk is resulting from a potentially damaging phenomenon and associated damage

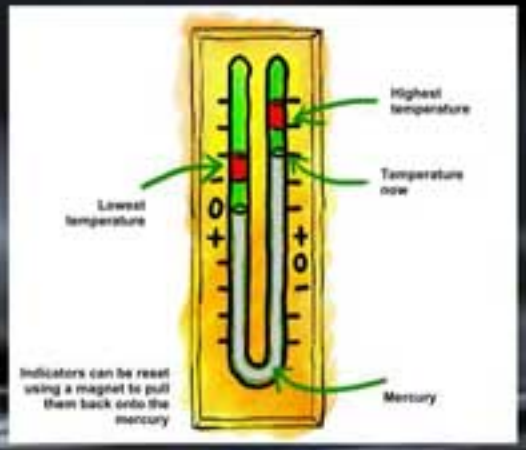
Risk= f (Probability, Consequences, Scenarios)

The susceptibility and resilience/survivability of the community / system and its environment to hazards

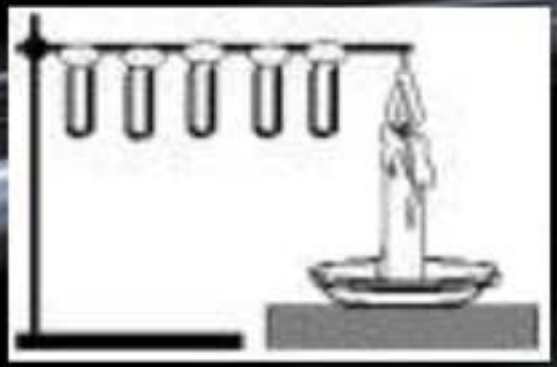
Vulnerability= f (Susceptibility, Resilience, State of Knowledge)

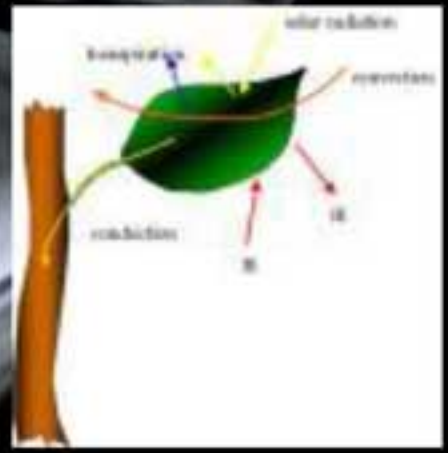
RISK IS NOT THE SAME AS VULNERABILITY!

TEMPERATURE



HEAT





QRA vs. QVA

QRA vs. QVA - at the root of this dis-symmetry is the common semantics.

Webster's Dictionary (v.e.g. the Landoll, Ashland, Ohio, U.S.A. edition, 1993) retains, in the entry for 'risk', the instrumental ingredients of the formula. Indeed, according to the said source, one has:

"Risk (noun). A chance of suffering or encountering harm or loss."

"Vulnerable (adjective). Open to physical injury or attack; (hence) vulnerability."

The Challenge

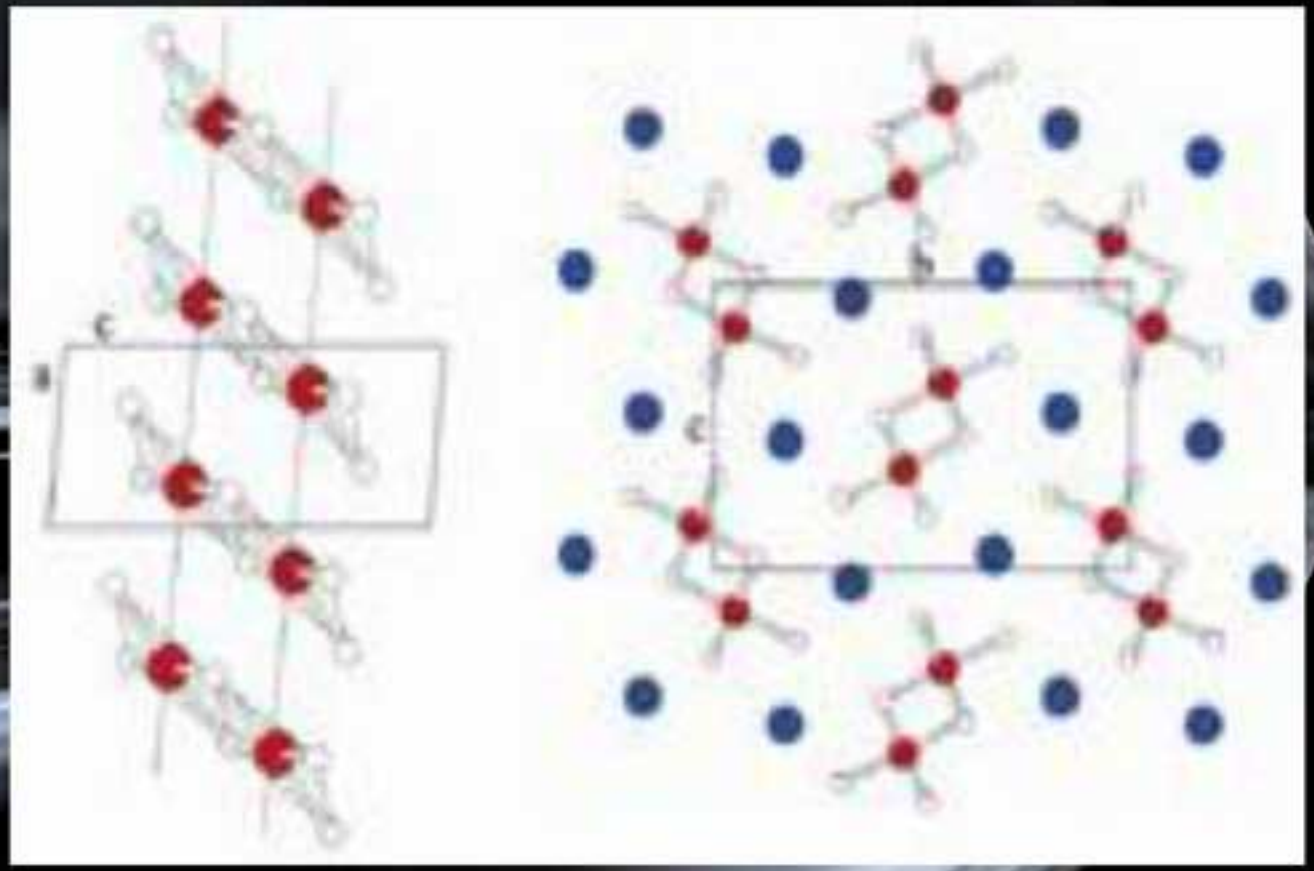
- The Quantitative Vulnerability Assessment (QVA) task is to take an **Adjective**, reflective of a virtuality ('Open To…') to a **Number**.

Achilles

Achilles, like all the warriors, was under ***Risk***, but his ***Vulnerability*** lead him to his death…

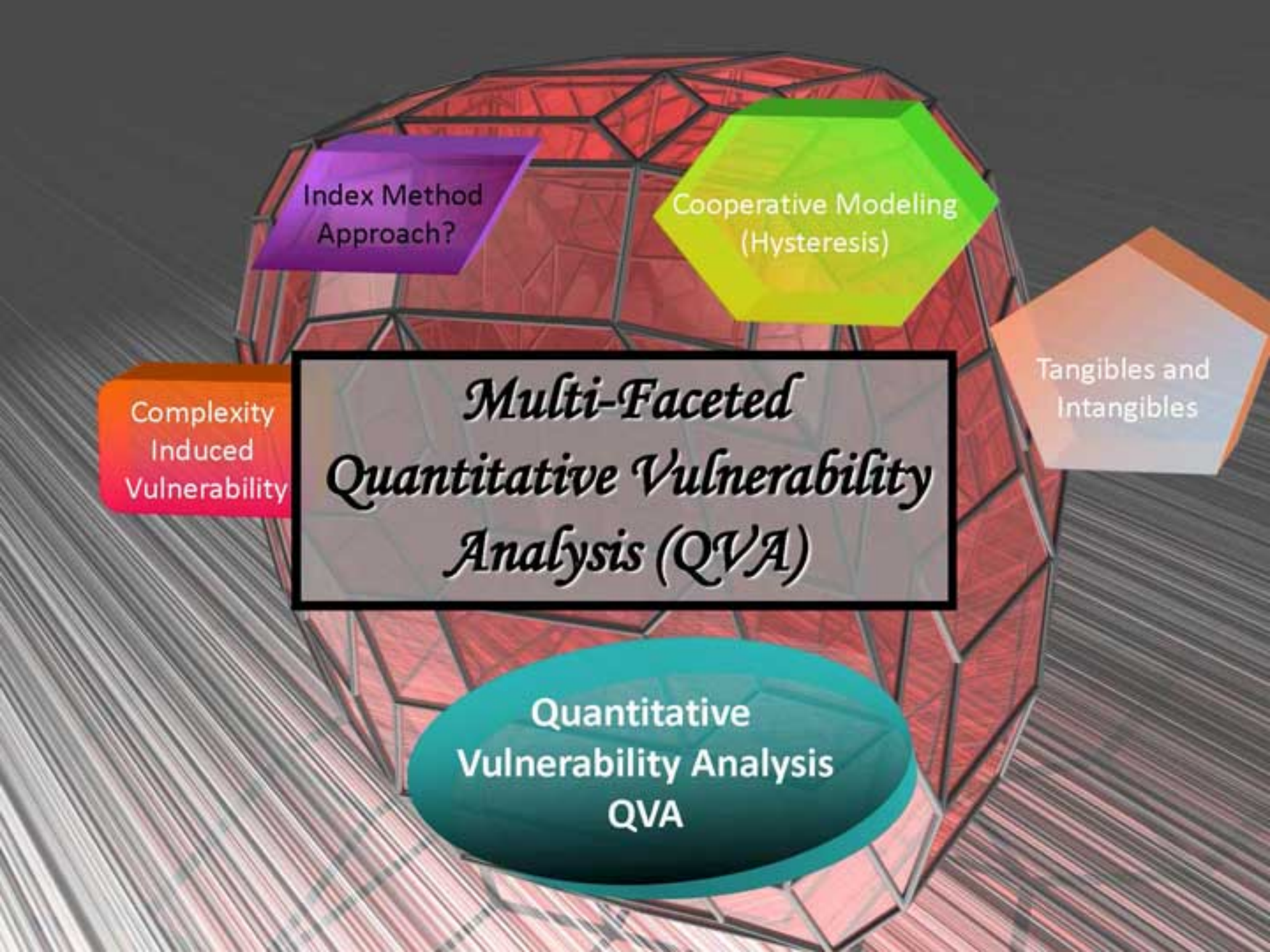
- *A*ddressing the following topics:
  - A quantification of the concept of vulnerability – ***need for a metric***
  - Defining and implementing a ***Vulnerability Event Scale*** for critical infrastructures
  - A ***Decision Support System*** for vulnerability assessment due to all hazard approach

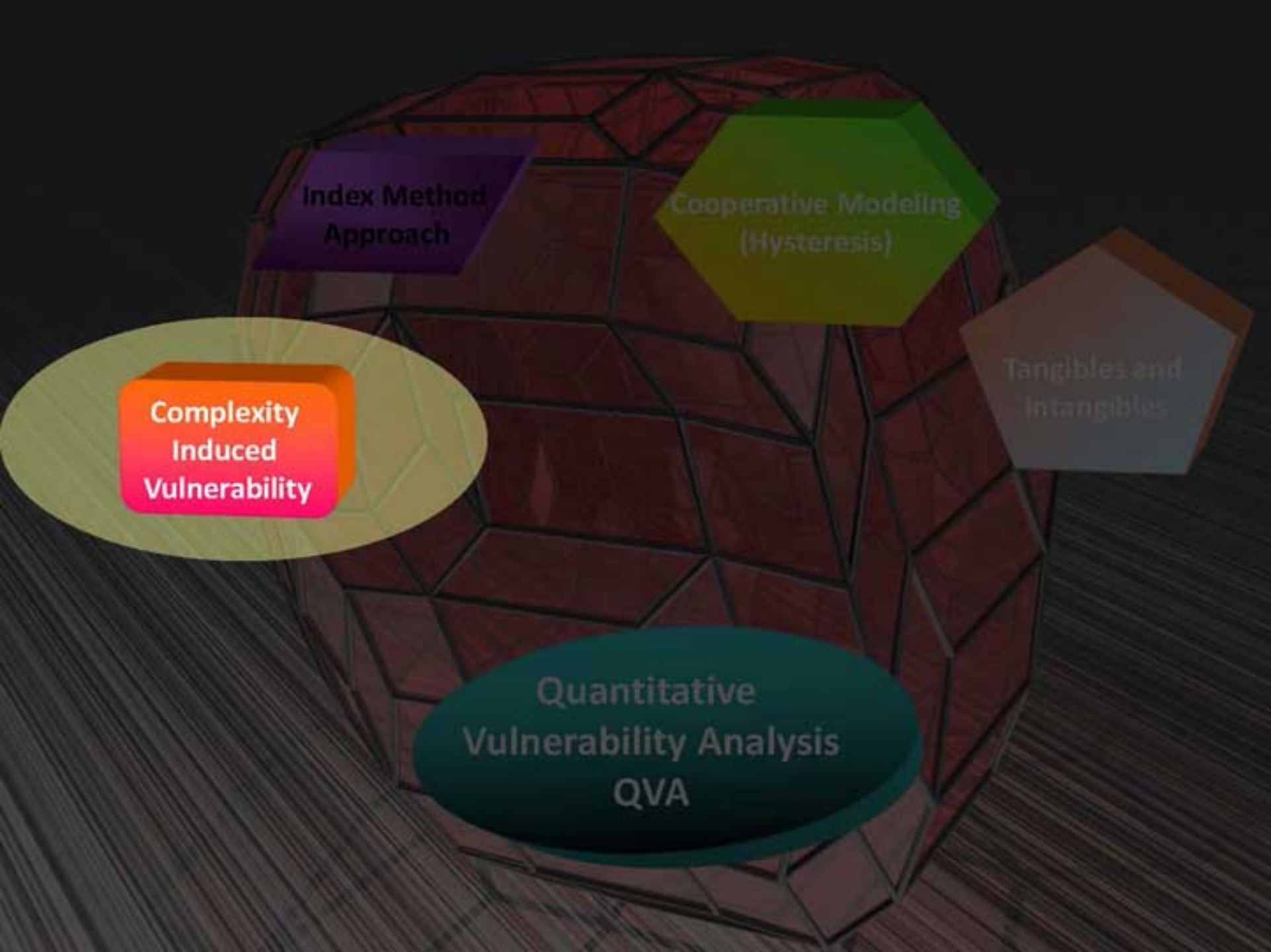
Comparative Vulnerability Assessment



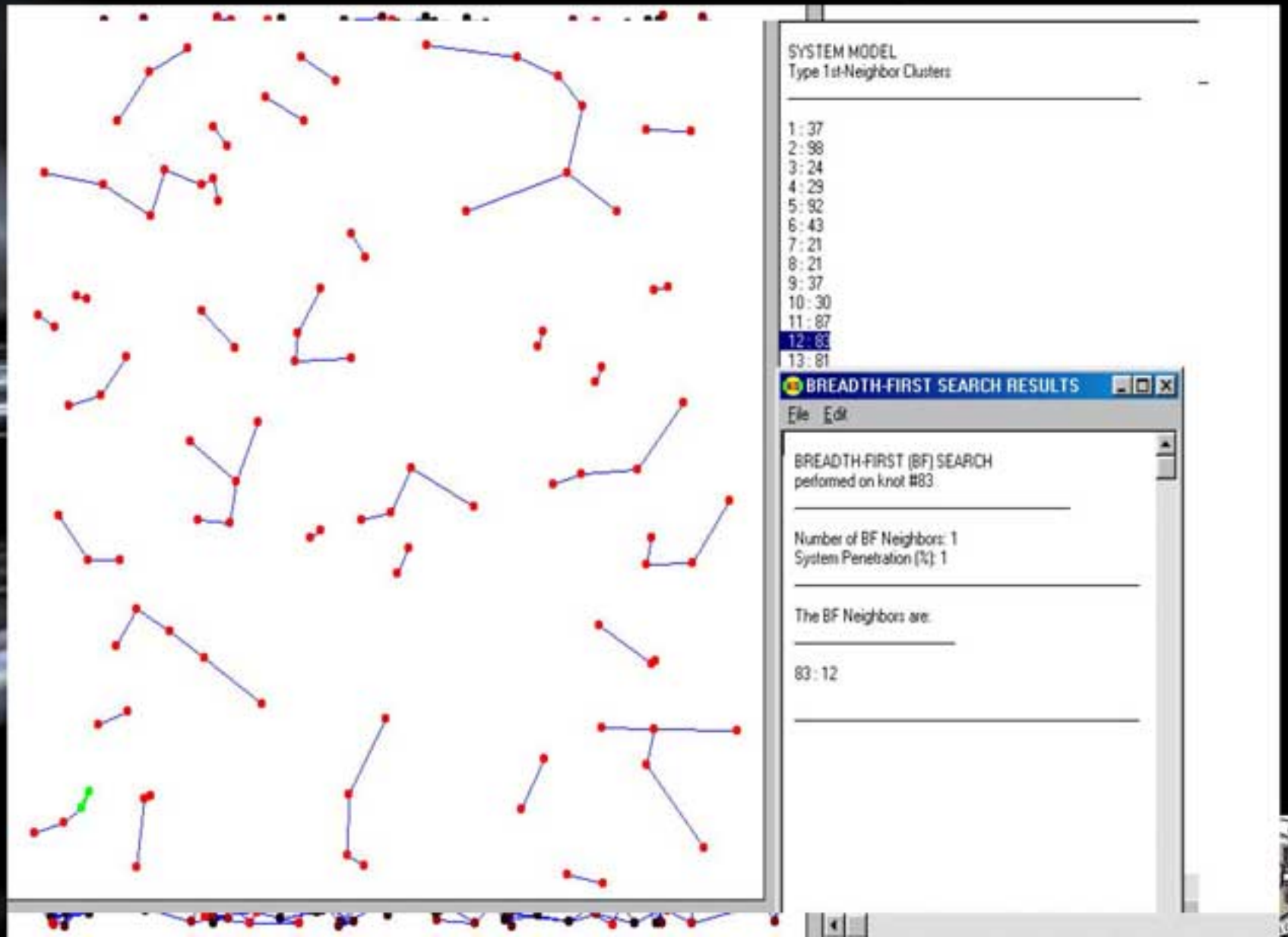
Part Two

Quantitative Vulnerability Assessment & Examples


Index Method Approach?
Cooperative Modeling (Hysteresis)
Tangibles and Intangibles
Complexity Induced Vulnerability
Multi-Faceted Quantitative Vulnerability Analysis (QVA)
Quantitative Vulnerability Analysis QVA


Index Method Approach
Cooperative Modeling (Hysteresis)
Tangibles and Intangibles
Complexity Induced Vulnerability
Quantitative Vulnerability Analysis QVA

Complexity Induced Vulnerability



- This work addresses a special line of thought, setting the task of taking *a straightforward approach to* ***complexity as a source of vulnerability.***
- The practical goal is to *attach a relevant metrics to* ***the internal connectivity of multi-component systems*** so that, this be turned to account from a *QVA (Quantitative Vulnerability Assessment)* oriented standpoint.

- ***Assumption 1:*** The operational representation of a multi-component system is a graph.

- The members, or constituents, or parts, of the system are the graph's ***knots***;
- The interactions of the members are represented by directed knot ***links;***
- The graph is customized to a system by attaching to knots a set of ***features,*** appropriately quantified and normalized on a vulnerability-relevant scale.

- ***Assumption 2:*** A higher internal connectivity in a system is a desirable quality only to the extent that the cumulated vulnerability relevance of the connected knots is tolerable.

- ***Assumption 3:*** The higher the vulnerability relevance of the knots involved in the exchange path of any knot of origin, including the relevance of the knot of origin itself, the higher the vulnerability induced in the overall system by the respective knot of origin; and

•***Assumption 4:*** The higher the cumulated vulnerability relevance of the system's knots, the higher the system vulnerability itself.

- Upon these, one may see that the attempt to characterize a system's vulnerability in terms of its 'complexity' should consider two distinct, if not completely independent, parameters:

System's penetrability - a quality that may have as a metrics the (average) number of knots that can be accessed starting from a (any) given knot in the system; and

The connectivity's ***vulnerability relevance*** depending on the penetrability defined above, yet also on the vulnerability relevance grades assigned to knot features.

The Model

The *individual vulnerability relevance*, *Vk*(*Ki*), of knot *Ki* :

$$V_k(K_i) = \sum_{j=1}^{N_f} W(F_j) \cdot G(F_j, K_i) \qquad (3)$$

The search-path (breadth-first) vulnerability relevance, *Vp*(*Ki*), of knot *Ki* and all the knots that can be accessed either directly or via other knots, into the system (index '*p*' for 'path'):

$$V_p(K_i) = V_k(K_i) + \sum_{m=1}^{N_i} V_k(K_m) \qquad (4)$$

The maximum possible vulnerability relevance of a system's knot:

Vmax = **max**(*Vk* (*Ki*)) . *Nk* = 9 **SW*(*Fj*).*Nk* =*9*1* Nk*

The *Average Vulnerability Relevance* per knot of system:

with *Vp* (.) given by equation (4).

$$V_{avg} = \left(\sum_{i=1}^{N_k} Vp(Ki)\right) / Nk \qquad (6)$$

One may also define the *Penetrability of the system from knot Ki:*

- *P*(*Ki*) = number of distinct knots that can be accessed from *Ki*,
- both directly and via other knots, plus *1* - the knot of origin

The *Maximum System Penetrability*, obviously given by

- *Pmax* = *Nk* (8)

The *Average System Penetrability*, per knot, given by:

$$Pavg = \left(\sum_{i=1}^{N_k} P(Ki)\right) / N_k \qquad (9)$$

Acceptability vs. Tolerability

'How tolerable the vulnerability of this system is':

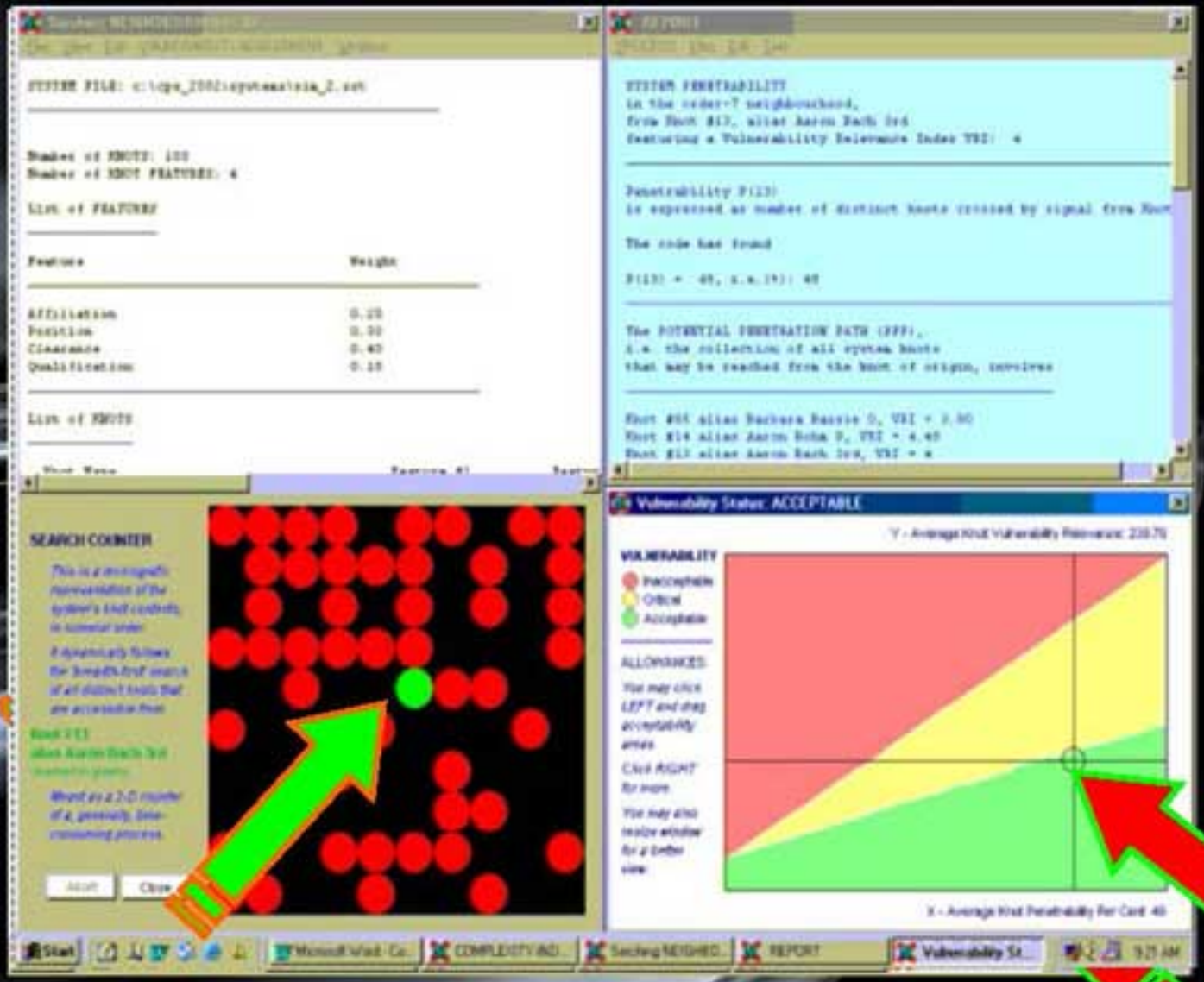
In the ***X-Y*** plane featuring

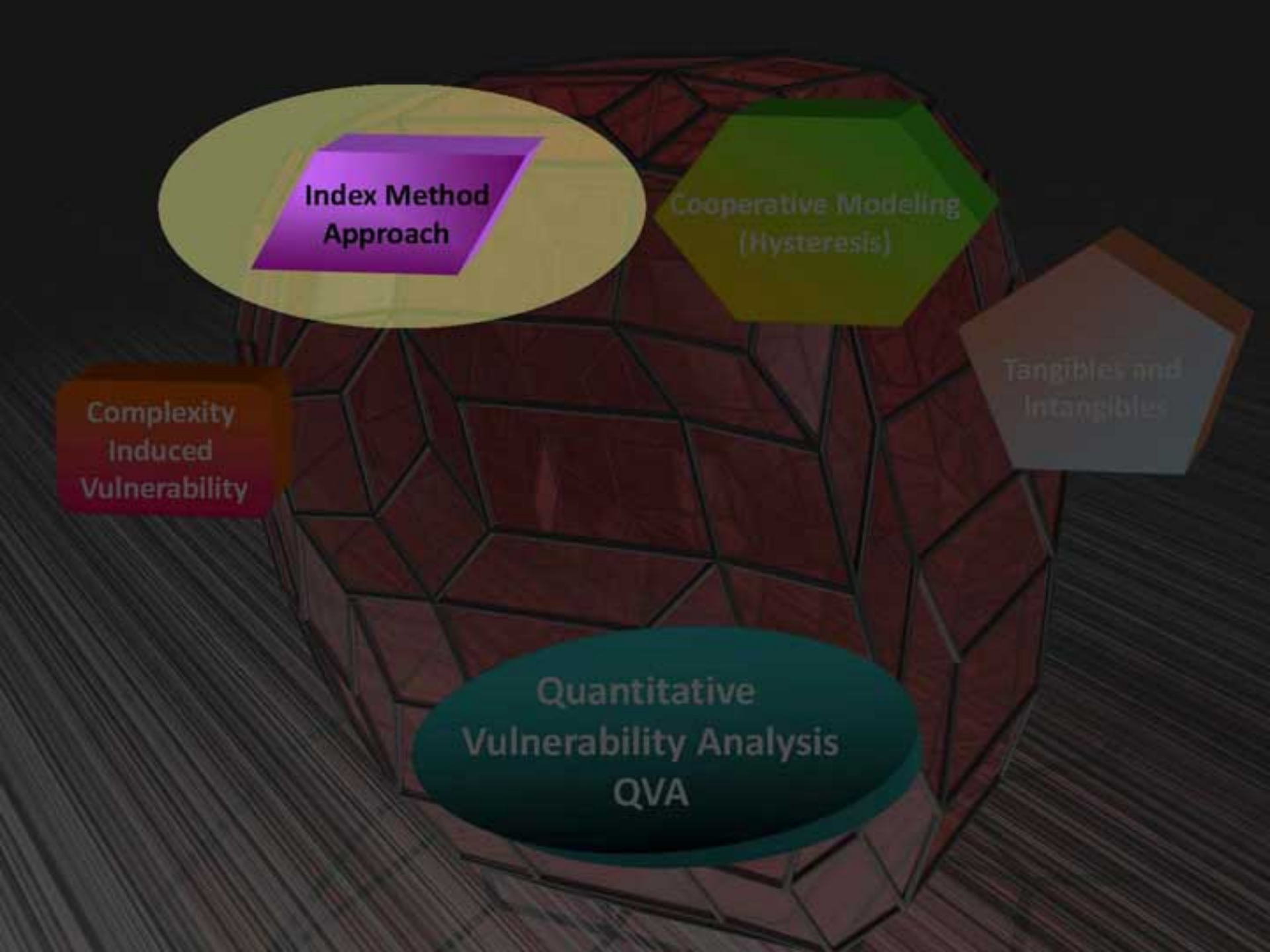
with the quantities involved given by equations above.

The ***X-Y*** space as defined above can be divided in, generally, 3 basins:

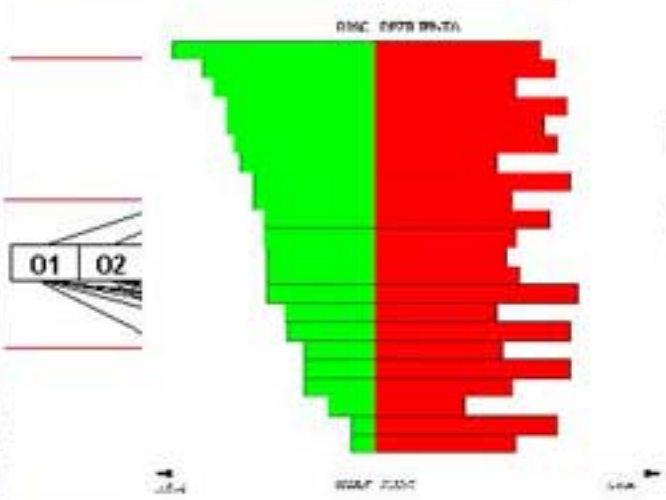
- the basin of ***Acceptable Vulnerability*** (green area)
- the basin of ***Critical Vulnerability*** (yellow area); and
- the basin of ***Inacceptable Vulnerability*** (red area);

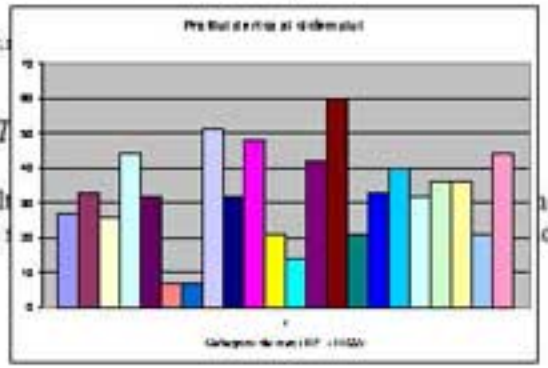
Complexity Induced Vulnerability Decision Support Systems

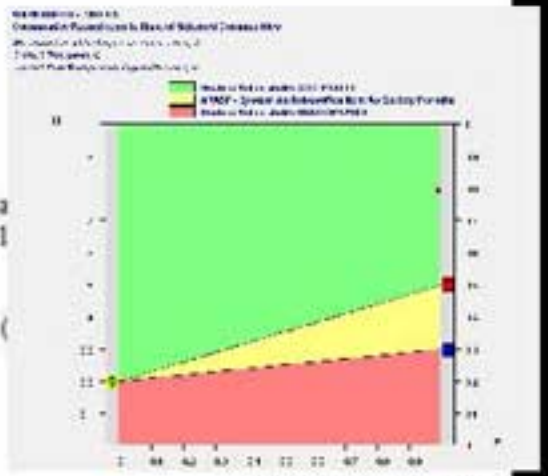



Index Method Approach
Cooperative Modeling (Hysteresis)
Tangibles and Intangibles
Complexity Induced Vulnerability
Quantitative Vulnerability Analysis QVA

Analytical Approach to Index Method Approach







14 - Instrumental

Nivelul 5,6,...

$$\sum_{i=1}^{m} w_i = 1 \qquad \text{(B.2.2.11)}$$

$$0 \le X_i \le 5$$

one gets

$$0 \le I \le 5$$

Problem Solver Equation

The System's *Vulnerability Index (V)* is defined with [illegible] *capability index* as [Gheorghe, 2003_4]:

$$V = 100 * \left(1 - \frac{I}{5}\right) \qquad \text{(B.2.2.12)}$$

The symbolic equation of computing the final weights is given in Fig. B.2.2.2.

Index Method Approach to Problem Solver Equation

$$I = \sum_{i=1}^{n_p} w_i X_i$$

I : The Risk Management Capacity Index

w_i : The Computed Weights of Instrumental Parameters

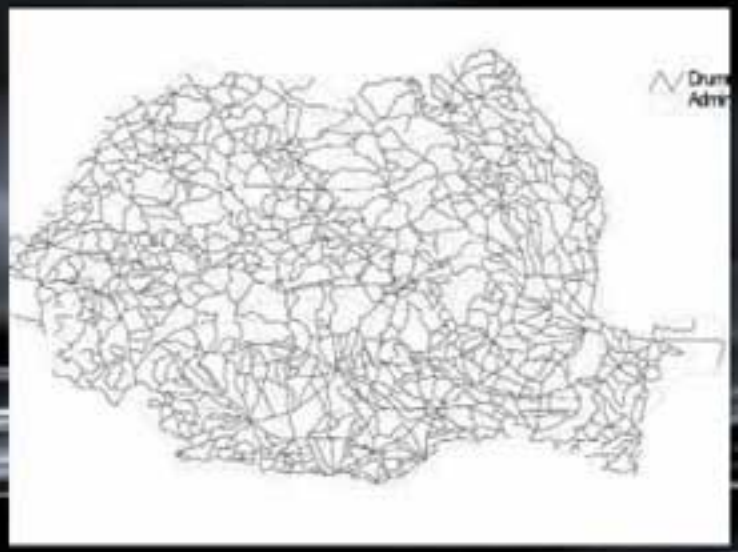
X_i : The Numerical Values (0,…5) of the Instrumental Parameter P_i

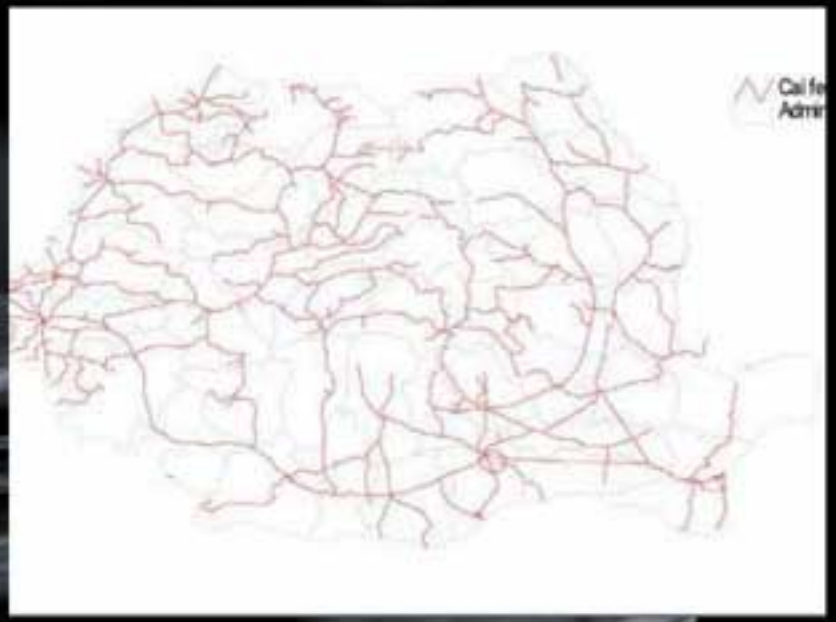
n_p : The number of Instrumental Parameters

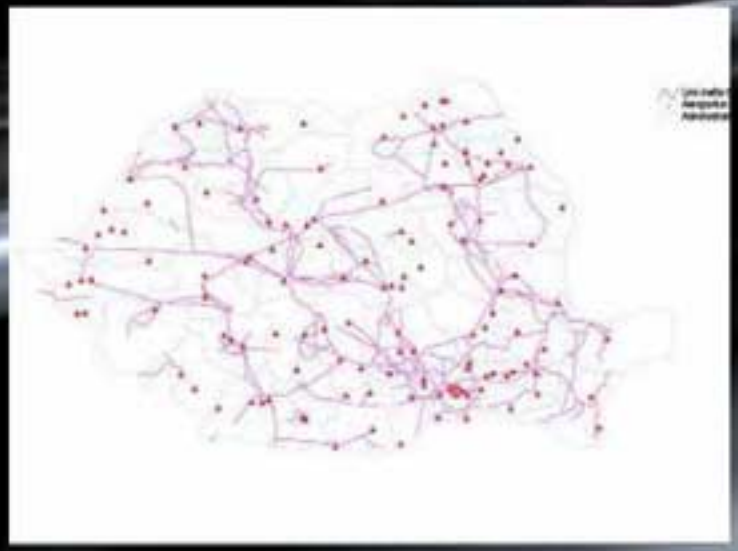
$$V = 100 \times \left(1 - \frac{I}{5}\right)$$

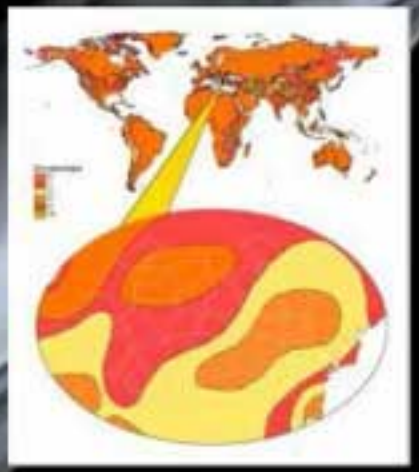
V : The Vulnerability Index of the System

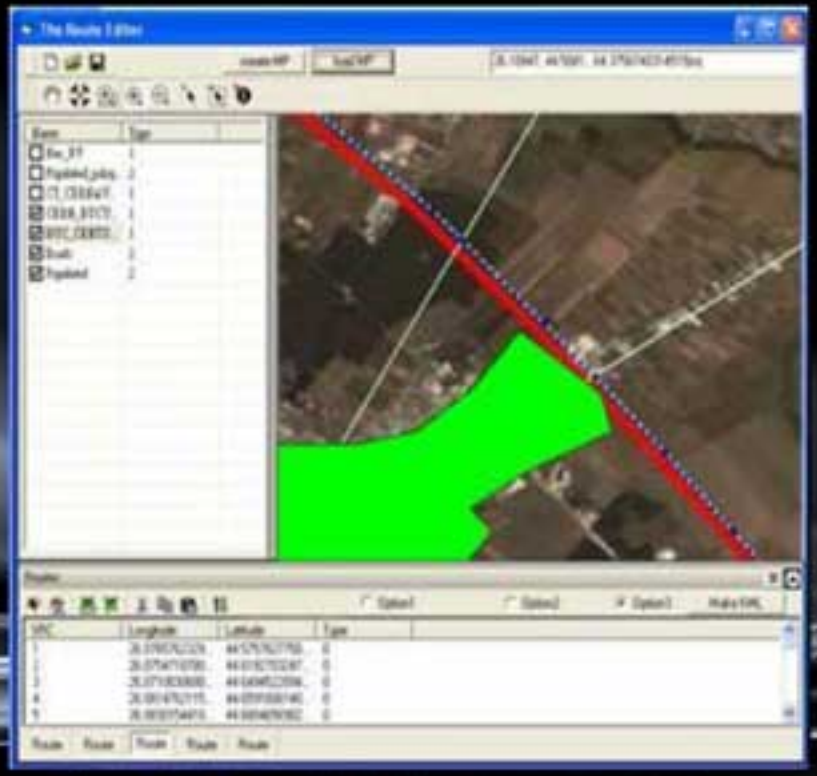
Corridor Selection TDG Example

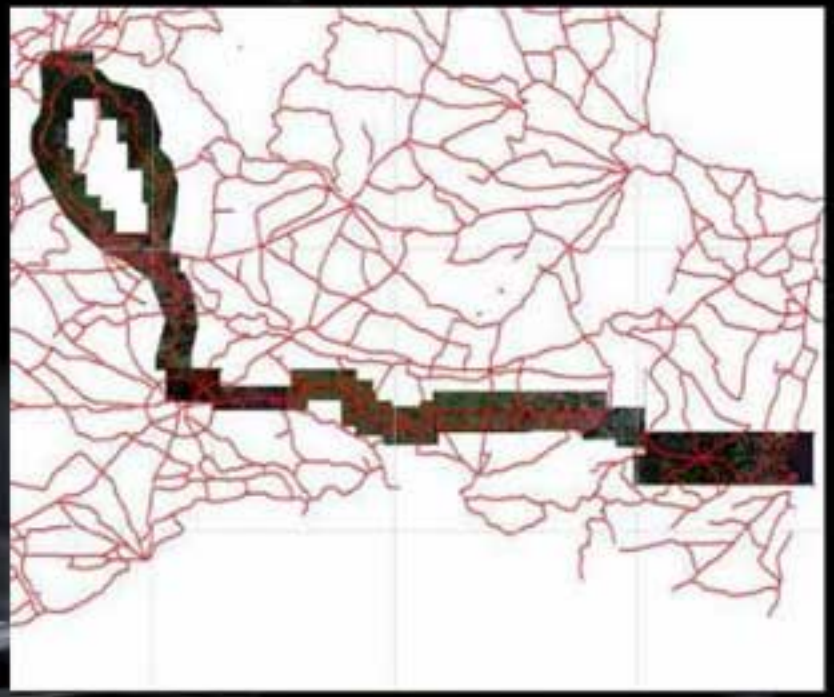












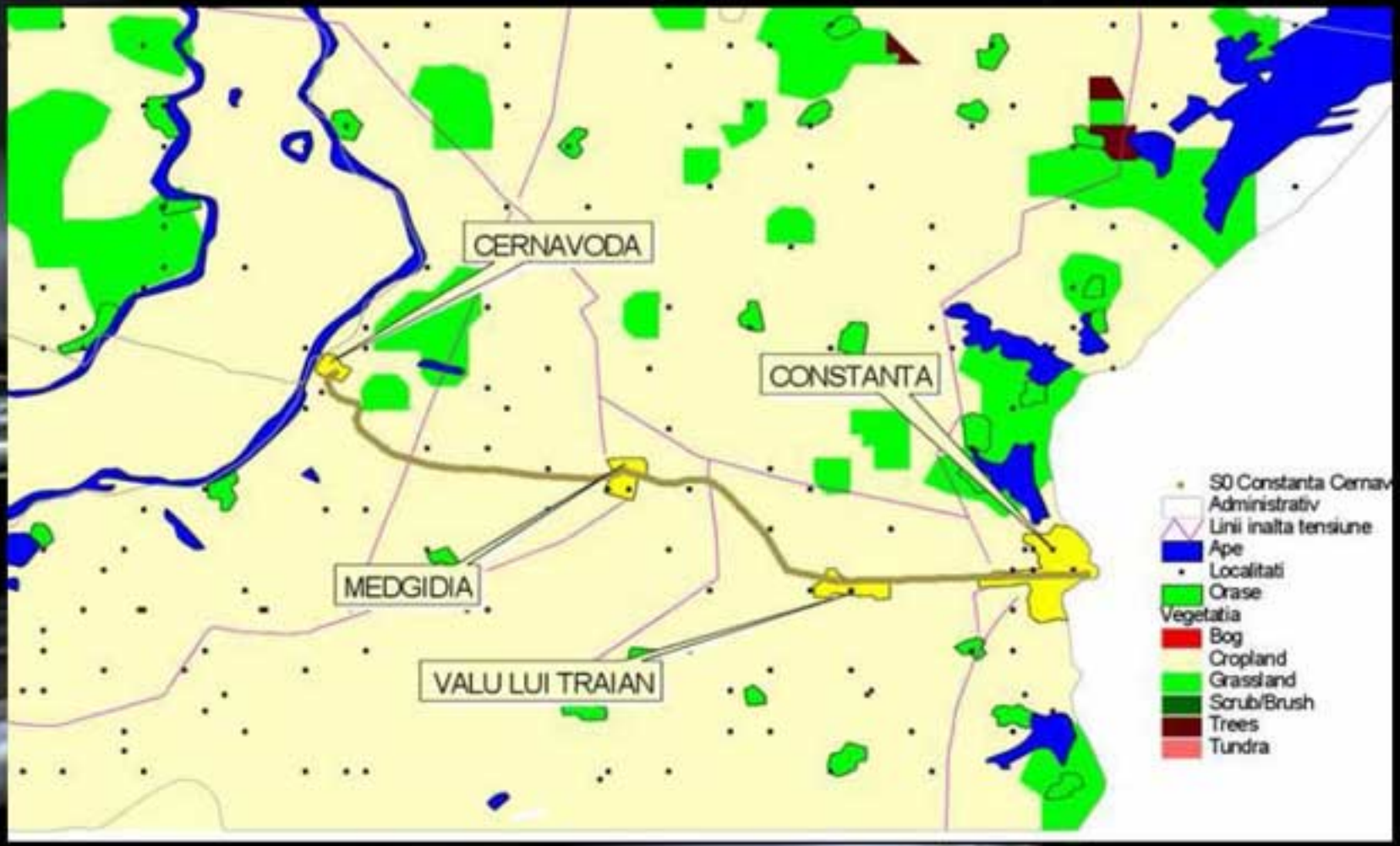
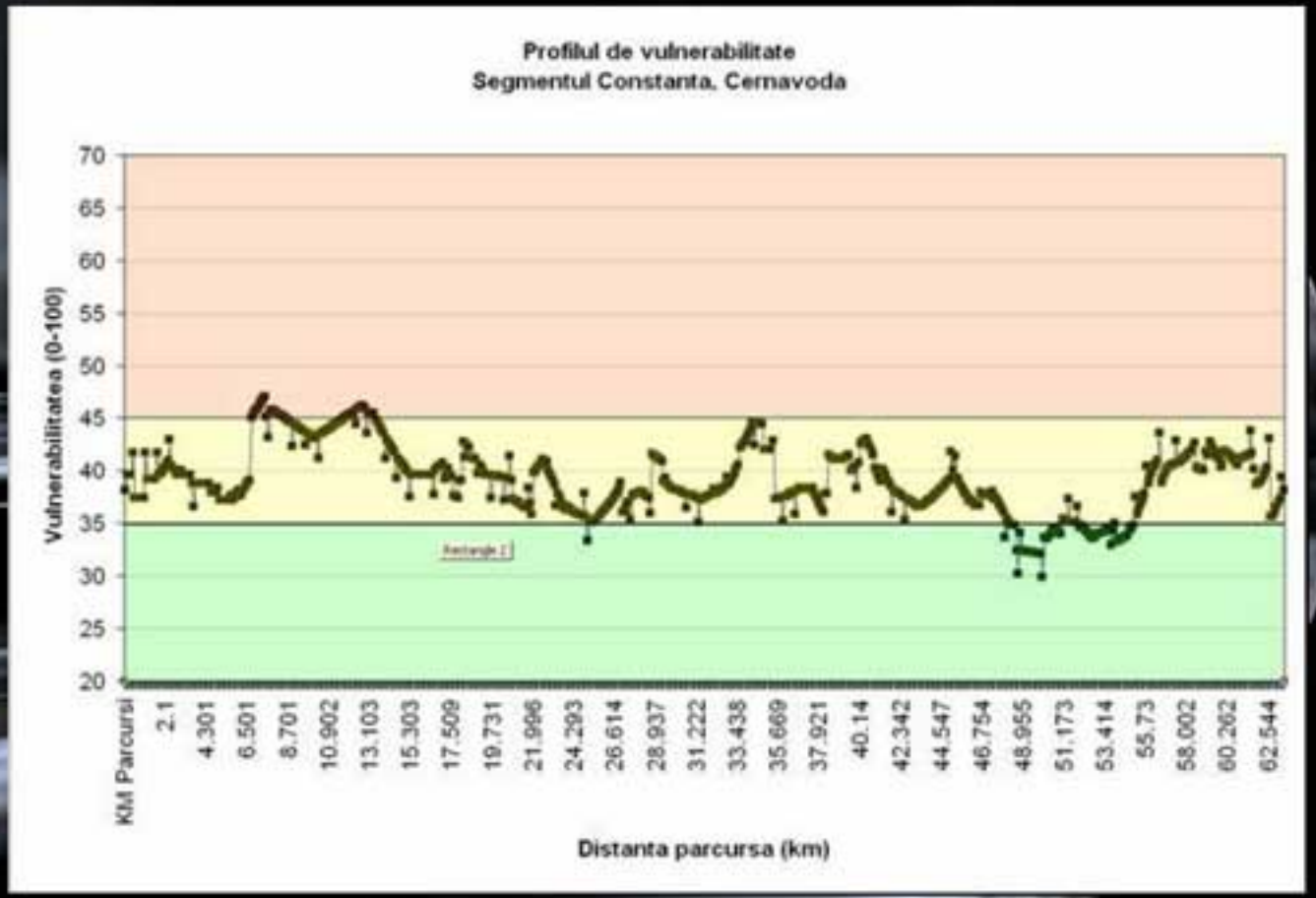
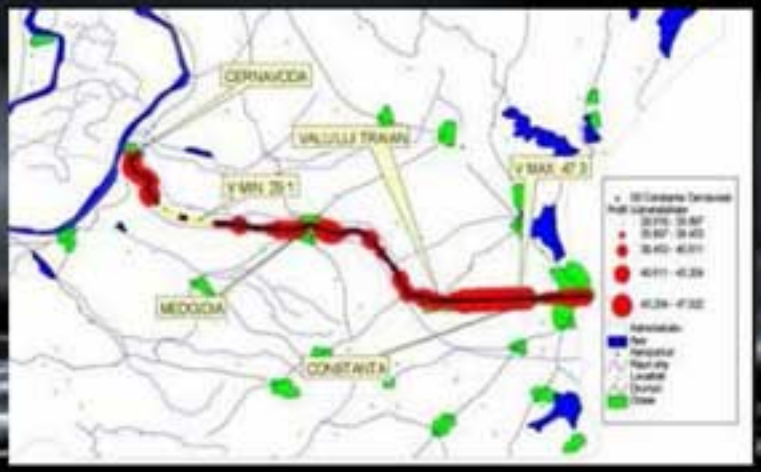

CERNAVODA
CONSTANTA
MEDGIDIA
VALU LUI TRAIAN
S0 Constanta Cernav
Administrativ
Linii inalta tensiune
Ape
Localitati
Orase
Vegetatia
Bog
Cropland
Grassland
Scrub/Brush
Trees
Tundra

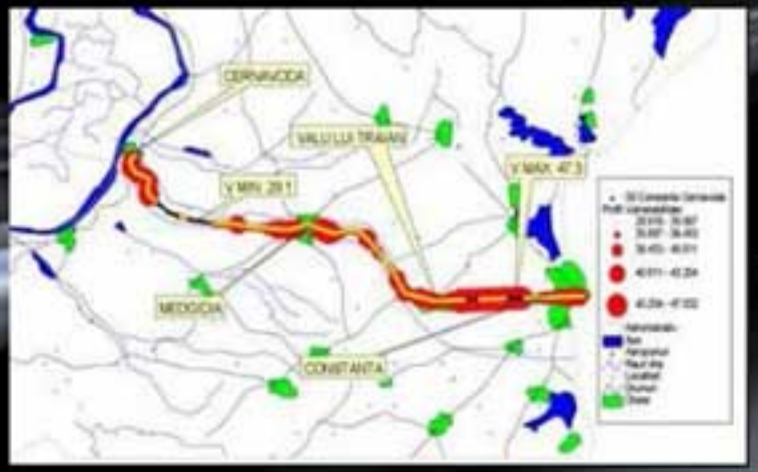

Image © 2006 TerraMetrics
Image © 2006 DigitalGlobe
© 2006 Europa Technologies
Google


Profilul de vulnerabilitate
Segmentul Constanta, Cernavoda
Vulnerabilitatea (0-100)
70
65
60
55
50
45
40
35
30
25
20
Km Parcursi
2.1
4.301
6.501
8.701
10.902
13.103
15.303
17.509
19.731
21.996
24.293
26.614
28.937
31.222
33.438
35.669
37.921
40.14
42.342
44.547
46.754
48.955
51.173
53.414
55.73
58.002
60.262
62.544
Distanta parcursa (km)

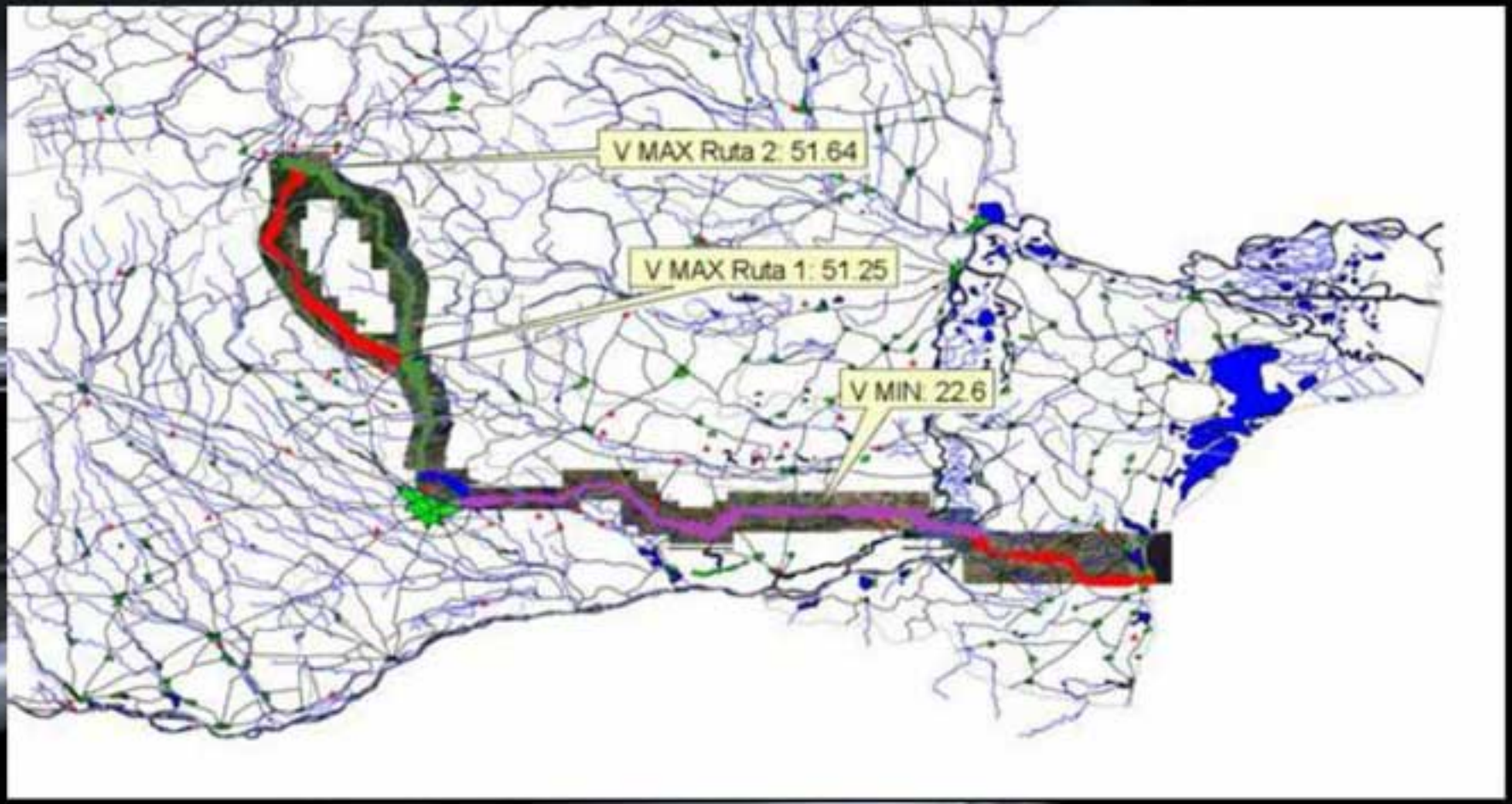
Vulnerability Profile:

Segment Constanta - Cernavoda

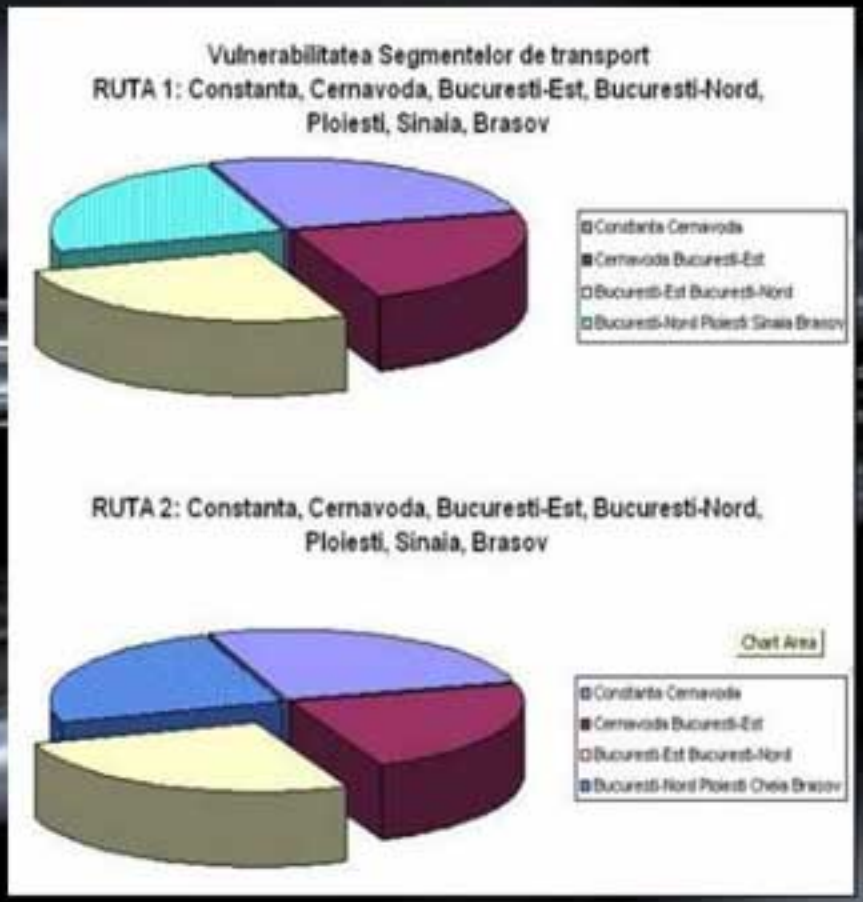


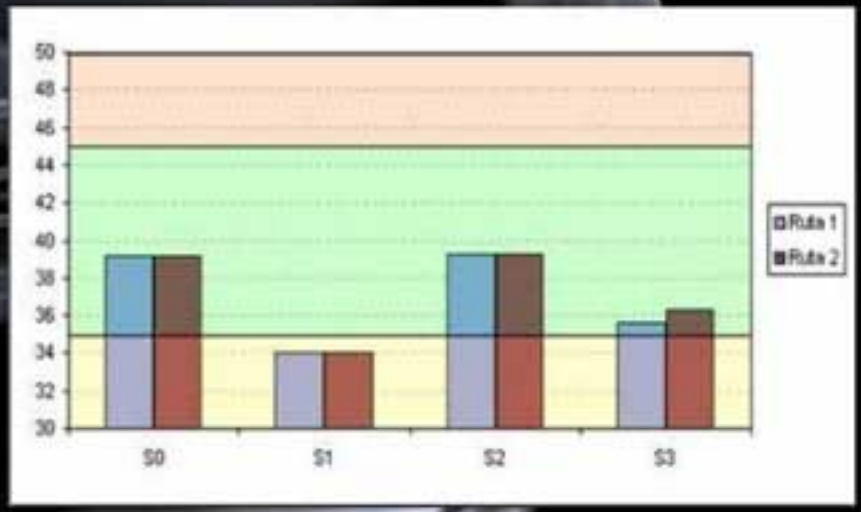


Vulnerability Profile for a Transport Coridor

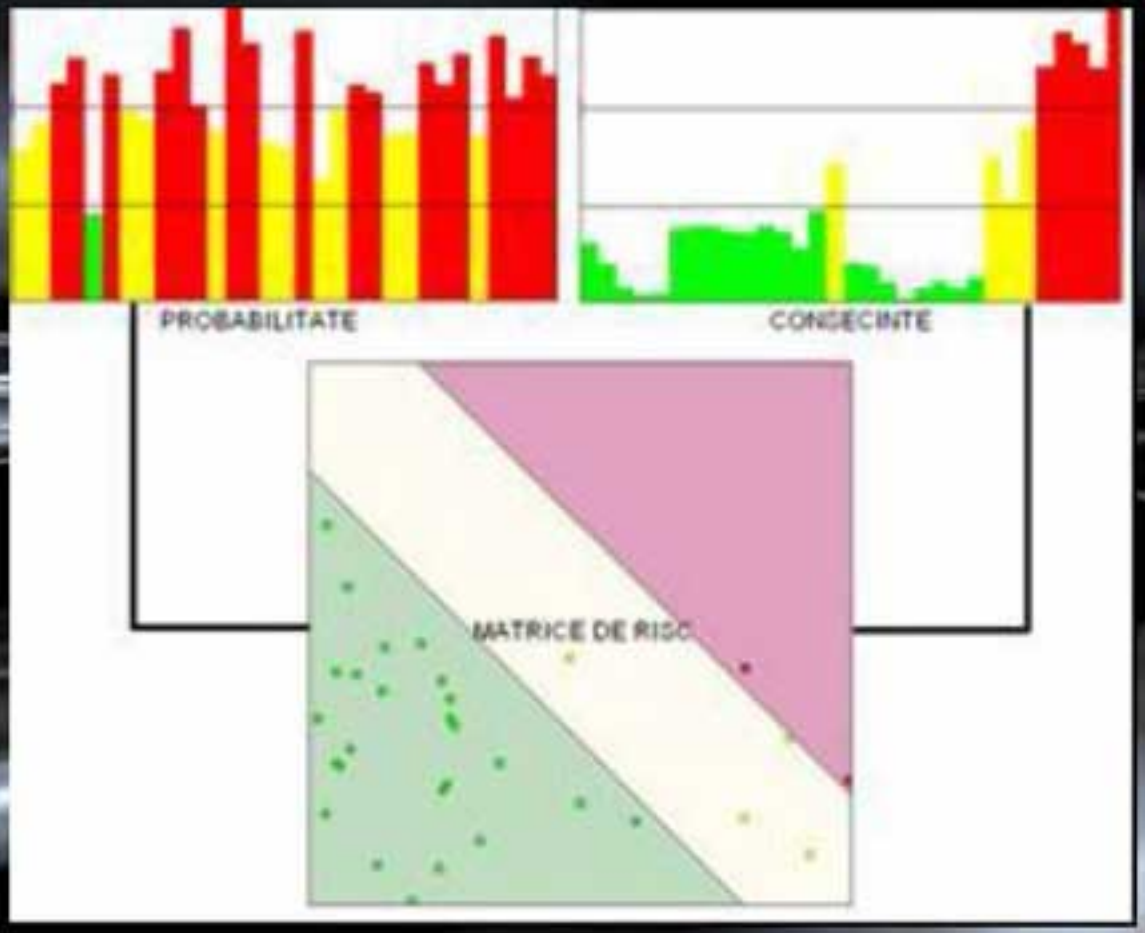


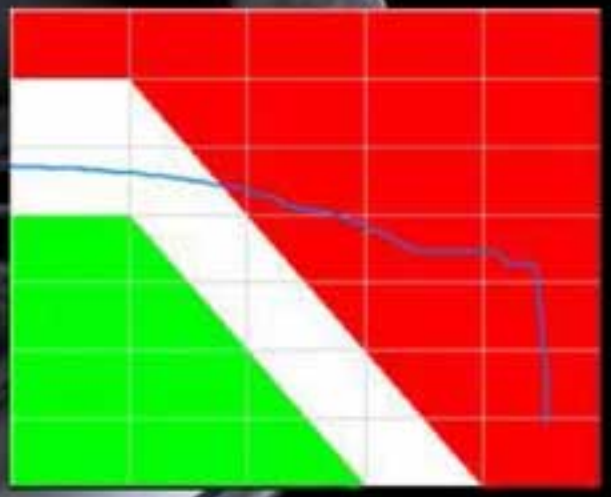
Comparative Results of Various Routes



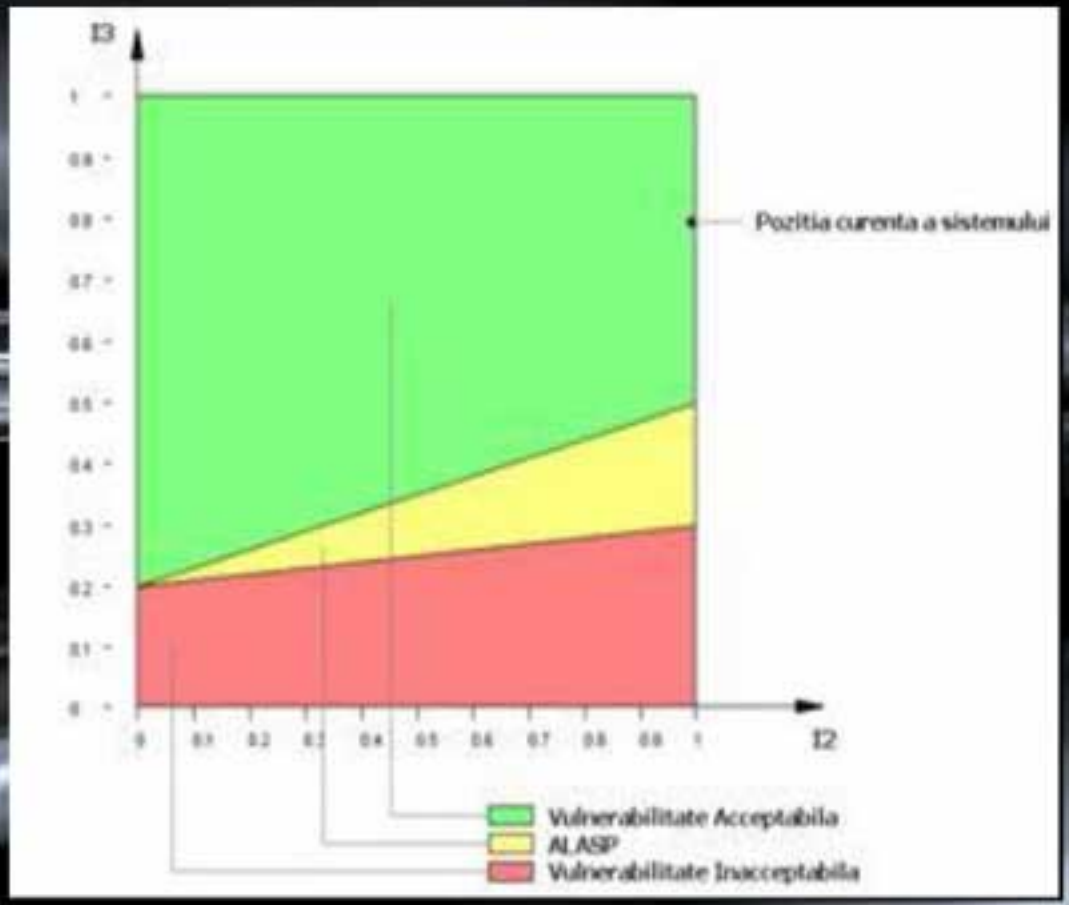


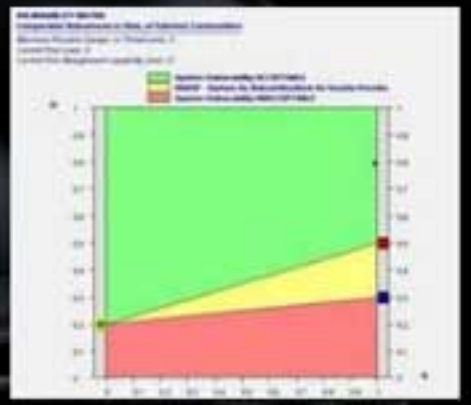
Risks and Critical Infrastructures

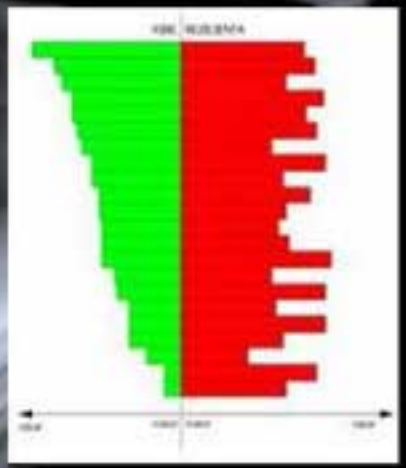




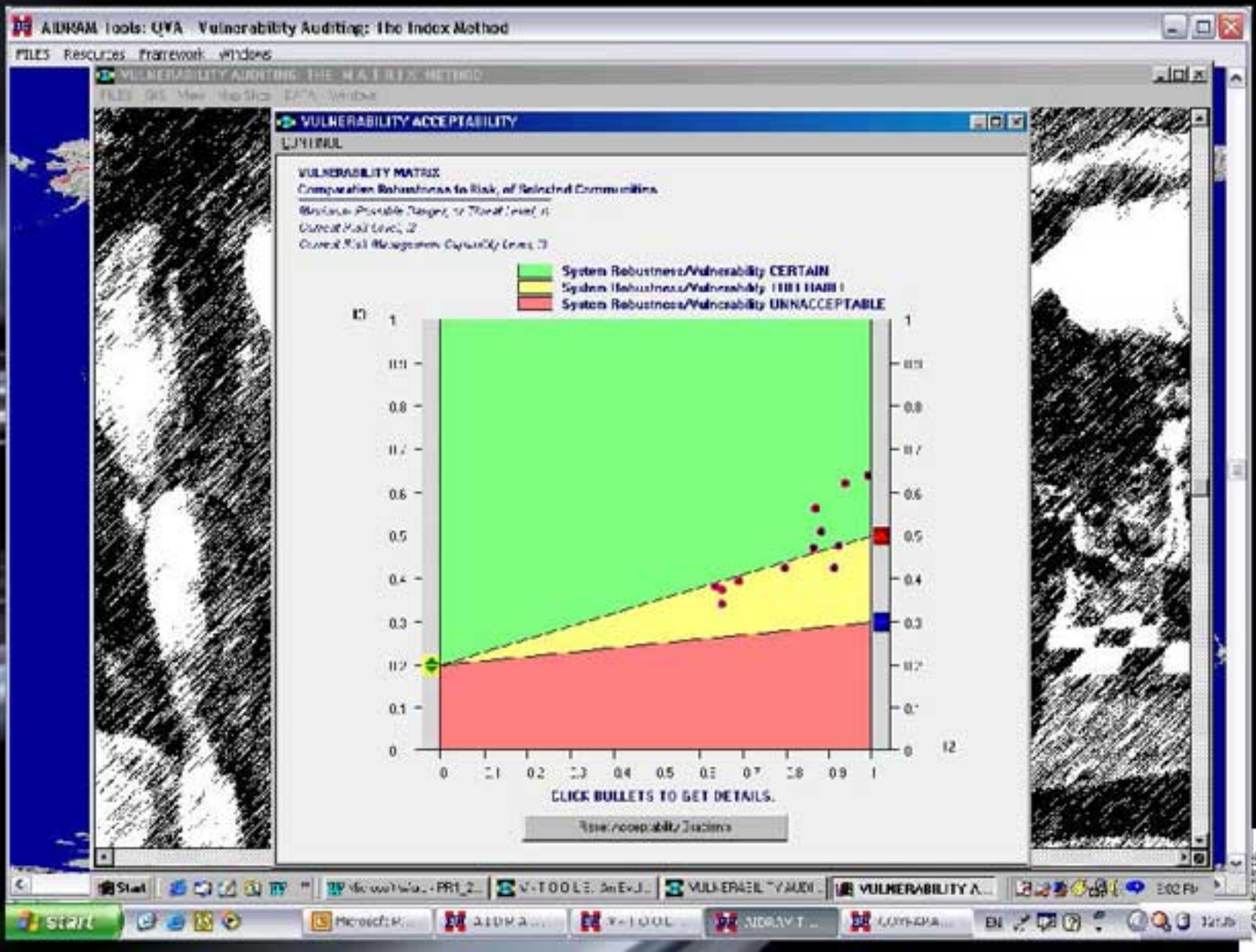
Vulnerability and Critical Infrastructures

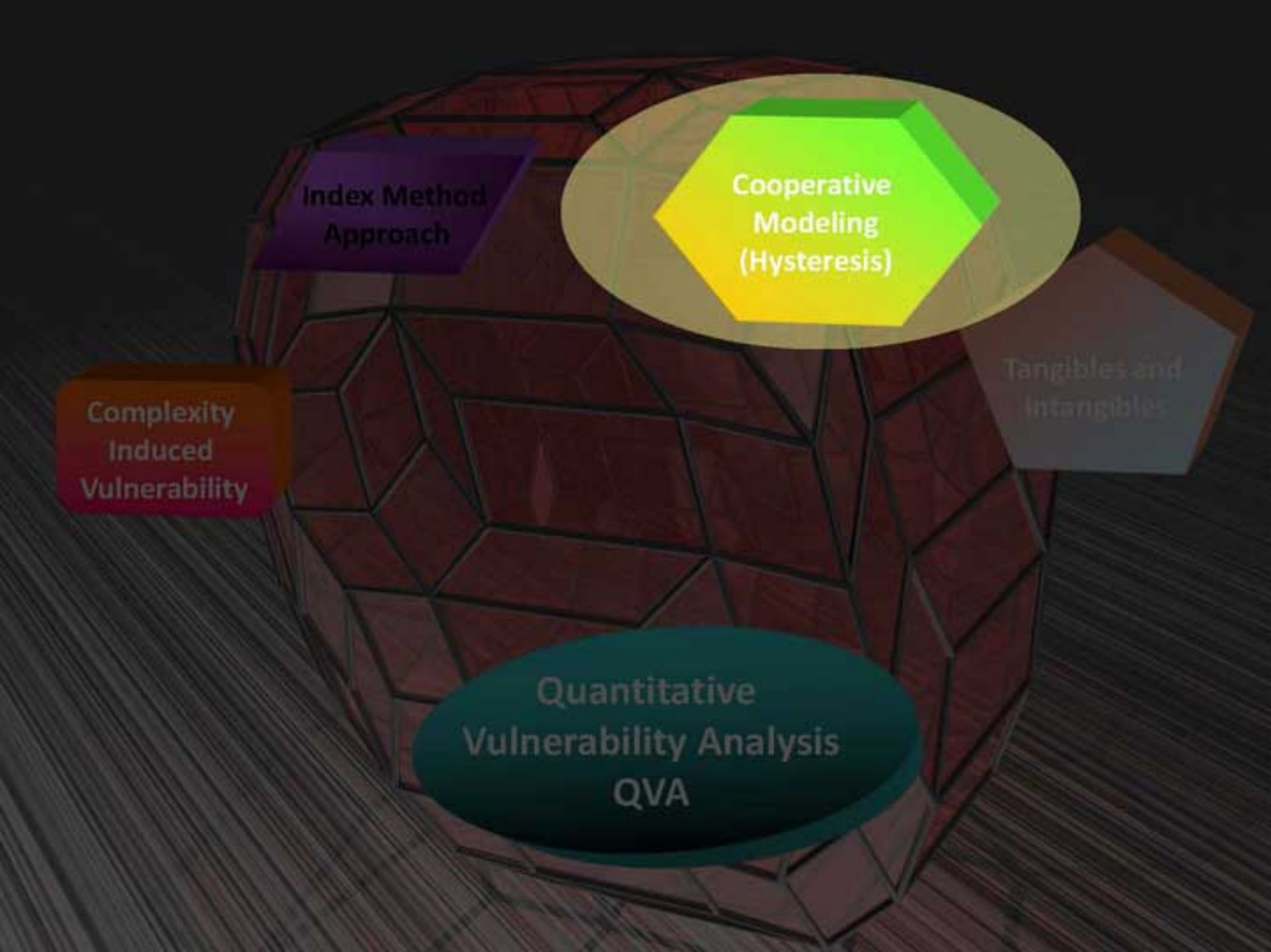






Numerical Evaluations




Index Method Approach
Cooperative Modeling (Hysteresis)
Tangibles and Intangibles
Complexity Induced Vulnerability
Quantitative Vulnerability Analysis QVA

On Hysteresis: Definitions

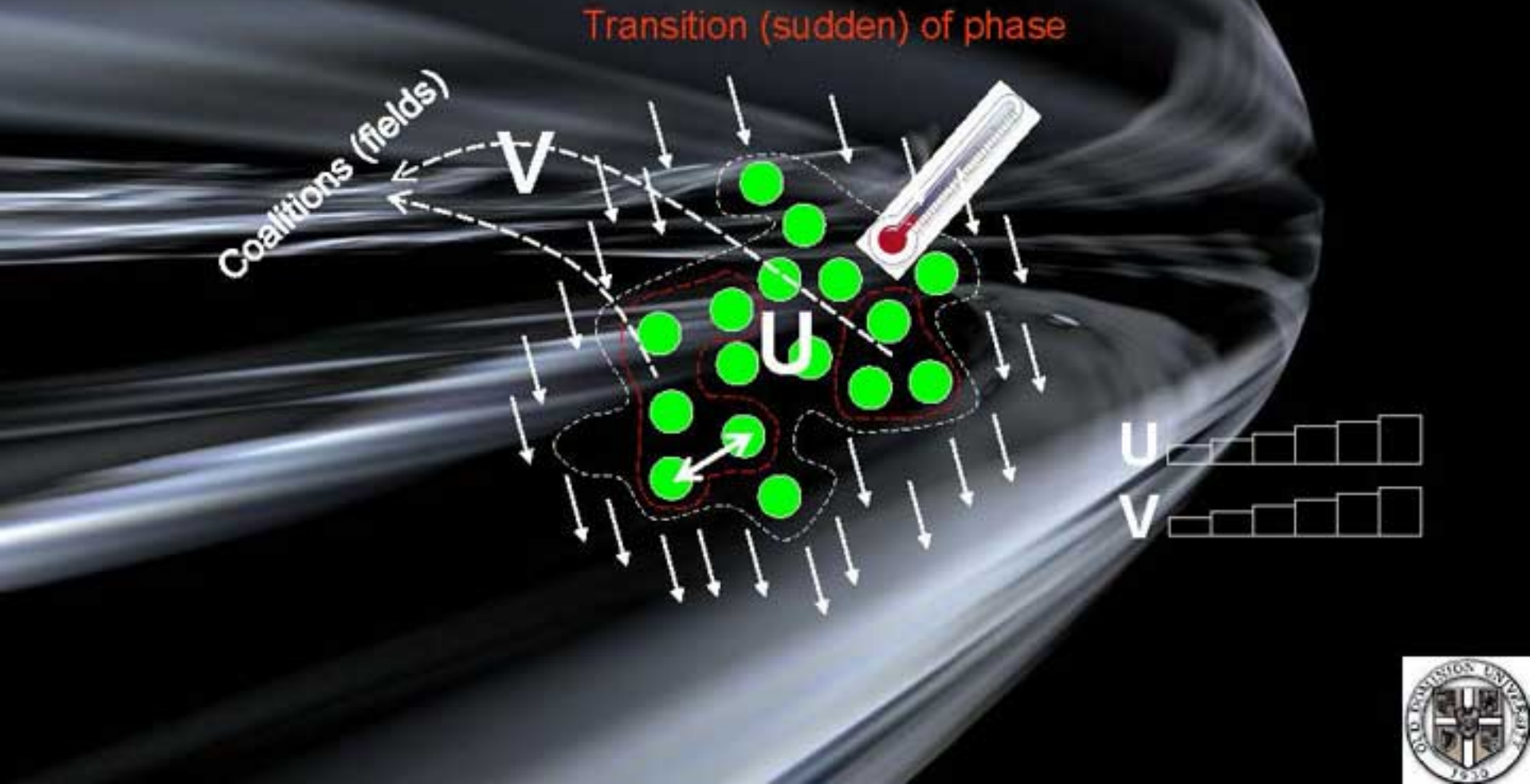
- The ***lagging of an effect behind its cause***; especially the phenomenon in which the magnetic induction of a ferromagnetic material lags behind the ... [Princeton]
- A property of a system such that an output value is not a strict function of the corresponding input, but also ***incorporates some lag, delay, or history dependence***, and in particular when the response for a decrease in the input variable is different from the response for an increase. ... [Wiktionary]

Model for consensual evaluation of vulnerability

Model based on physical analogies

Model for consensual evaluation of vulnerability

Model based on physical analogies



Cooperative Modeling: Vulnerability of Critical Infrastructures

- A two-parameter description and the respective equation of state, for any multicomponent, multi-indicator system featuring two states: 'operable' and 'inoperable'
- A division of the two-parameter phase space of the system into 'vulnerability basins'; and
- A 0-to-100 'Vulnerability Scale', and the means to measure the respective 'Vulnerability Index', as an operational expression of a 'Quantitative Vulnerability Assessment' (QVA).

A method to diagnose the current vulnerability of a complex system featuring large numbers of indicators, both internal and external, as well as to dynamically monitor the time-evolvement of the vulnerability as the indicators change, is demonstrated.

A Consequent Algorithm and Its Software Implementation

The method, algorithm, and software are *Generic*,
and are believed to accommodate a virtually unlimited variety of applications.

The notions are inspired by reference frameworks
in classical *Statistical Physics* such as the Bragg-Williams approximation of the Ising model (v.e.g. Huang), feed from the alternative interpretations by Thom and Zeeman, of the *Stability problem in Systems Theory*, and are encouraged by the similar approaches by Hacken, Weidlich and others.

System Is 'Unstable', or 'Prone To Collapse'

The cusp line, plus - at normal-to-higher 'temperatures' - a segment of the V = 0 line make up a 'maximal vulnerability line' in the (U, V) plane. The model will take that, for the system, reaching the V = 0 line means its collapse - the system becomes **inoperable**.

While for U < Ucusp line the assumption above looks natural - the system state enters, with certainty, the 'system inoperable' quadrant of the cusp foil, at higher U one can only say that the system may collapse down to the " system inoperable" part of the foil. In other words, the ***system is 'unstable', or 'prone to collapse',*** or indeed - ***'vulnerable',*** and the more so, the higher U.

Assumptions

Assumption 1: Vulnerability: a system's virtual openness to loose its design functions, and/or structural integrity, and/or identity under the combined interplay of two sets of factors:

U - *System deficiency factors (internal)*; and
V - *Management deficiency (external) factors*.

All factors are supposed to be quantifiable by appropriate indicators.

U-factors feature the proneness of the system to disruptive developments. The associated indicators cover features that are *internal* to the system. They are fast-variable indicators.

V-factors feature the capability of the system's management to react/respond to internal developments within the system. Such factors feature the ambient in which the system evolves; they are, mainly *external*. They appear to be, in comparison, slow-variable indicators.

Assumptions

Assumption 2: The ensuing assumption is that system's measurable /monitored indicators (parameters) may indeed be aggregated such that two control variables U and V be, respectively, obtained.

In consideration of their nature, one submits that U and V are membership functions of the ***fuzzy theory approach*** to impact Indicators

Accordingly, if Xi , i = 1, 2, ..., n are the normalized indicators contributing in the definition of U, then one has:

$$\mathbf{U(u_1, u_2, ..., u_n)} = \min(1, (X_1^p + X_2^p + ... + X_n^p)^{1/p})$$

A similar set of equations would give $\mathbf{V (v_1, v_2, ..., v_n)}$

Indicators for Vulnerability Assessment

Loss prevention	2-4	Contractor, Third party services	3-4	Operating-, emergency procedures, P&IDs	4-4	Emergency plan	5-4
2-4-1. Fire water supply		3-4-1. Area and extend of subcontraction		4-4-1. Operating, emergency, P& ID, & upgrades		5-4-1. Emergency plan	
2-4-2. Fire brigade		3-4-2. Contractor Selection		4-4-2. (Equipment) Shutdown / restart procedure; & PSSR			
2-4-3. Manual firefighting system process units		3-4-3. Contractor Training					
2-4-4. Fixed firefighting systems process units							
2-4-5. Fire detection system							
		control		maintenance			
		2-1-5. Flood protection		3-1-5. Number of leaks , spills (trend)		4-1-5. Safety meetings, committees	

Assumptions

Assumption 3: In a conventional sense, an operable system may thereby appear as:

- *Stable,* and thereby featuring a *low vulnerability*;
- *Critically unstable/vulnerable*; or
- *Unstable,* and thereby featuring a *high vulnerability*.

Beyond these, the system may only be found inoperable.

The model includes a *Markov probabilistic model* which incorporates probabilities in order to estimate vulnerability, on a generic stage.